



Managing Expectations and Job Satisfaction

FOR IT SECURITY LEADERS



Contents

Job satisfaction is vital to consistent performance	4
Tensions run high for cybersecurity decision-makers	5
Most security leaders are open to new positions	6
Good relationships with senior leadership are a strategic priority	7
Stress-related issues rarely remain isolated for long	8
Organizations can do more to support security leaders	9
Cybersecurity leaders routinely put in overtime	10
Practical stress support goes a long way	11
Reduce stress while improving operational security performance	12
Research at-a-glance	13
Methodology	14

BlackFog research shows
where job-related stress has
the highest impact on security
leaders' performance.

1

Job satisfaction is vital to consistent performance

Cybersecurity decision-makers have wide-ranging responsibilities. They are not only accountable for preventing cyberattacks and malware, but also for implementing solutions that maintain productivity and usability. The need to balance security and usability often puts CISOs and other security leaders in conflict with other C-suite executives.

This conflict can have negative repercussions. Security leaders may feel that mission-critical initiatives are not given sufficient priority by the company. When cybersecurity incidents occur, they are nevertheless held personally liable for the failure. This impacts job satisfaction and reduces the incentive to proactively improve security

performance moving forward.

BlackFog has conducted research into how security decision-makers navigate these unique stress factors. These findings will help security leaders and board members proactively address common tensions and align security operations with broader business goals.

2

Tensions run high for cybersecurity decision-makers

Malware, phishing, and supply chain attacks are among the chief concerns cybersecurity leaders address in their day-to-day operations. At the same time, they must prepare for emerging threats, like cybercriminals using AI to launch increasingly sophisticated assaults at little-to-no cost.

These stress factors are amplified by preventable internal tensions. In the United States especially, there is a trend towards prosecuting individual security leaders for their personal culpability in cybercrime incidents. This puts an additional layer of pressure, backed by potential criminal liability, for a job that fundamentally involves managing unknown risks.

Personal liability is the subject of healthy debate between cybersecurity professionals. Roughly half of our survey's respondents believe personal liability improves accountability for security leaders. The other half worries that it will deter motivated and competent people from seeking leadership positions altogether.

3

Most security leaders are open to new positions

The combination of emerging threats, funding difficulties, and personal liability is increasingly convincing security leaders to seek new positions. One out of every four respondents claim they are actively looking for a role in a new organization. Another 54% claim they are open to new offers. Altogether, the majority of security leaders would take on a new role if given the chance.

The vast majority of those considering new employment say the stress and demands of their current role have contributed to their decision. They don't feel empowered to improve the organization's security posture or risk profile. At the same time, they fear being held personally responsible for security failures when they occur.

Nearly half of security leaders who report actively looking for a new role say they don't see eye-to-eye on

major issues with senior leadership. Security leaders who feel their professional opinion is ignored by senior leadership are more likely to work at mid-sized organizations with between 1000 and 4999 employees.

When asked when they would consider leaving their current organization, the average length of time reported was nine months. One-quarter of respondents said they are "not sure" when they would leave.

4

Good relationships with senior leadership are a strategic priority

Respondents actively searching for new roles at other companies tend to report poor-quality relationships with senior leadership. They are more likely to say the Board does not see eye-to-eye with them on the most pressing issues, which increases stress and tension while contributing to fear of personal responsibility.

Security leaders who have difficult relationships with senior leaders are more likely to report feeling under pressure, and have a negative outlook on the trend towards holding CISOs personally liable for security event outcomes. These issues have a direct impact on the organization's security posture, and should be addressed proactively.

Effective relationship management between security leaders and Board members is crucial for consistent security performance. Cybersecurity

leaders who have more access to the company's Board are more likely to report job satisfaction than those who encounter barriers between themselves and senior leadership.

Overlooking security in leadership meetings can expose the organization to preventable risks and impede the integration of cybersecurity initiatives across the company. Giving CISOs a seat at the table is the first step towards achieving reliable long-term success with security initiatives.

5

Stress-related issues rarely remain isolated for long

Many cybersecurity decision-makers report taking steps to relieve stress and improve their work-life balance. Some turn to hobbies and sports activities to maintain a healthy outlook and set boundaries between their personal lives and work. However, others admit engaging in concerning behaviors like self-isolating from social activities or using drugs and alcohol.

Anyone who engages in antisocial behaviors risks letting the consequences of those behaviors spill over into their professional life. These impacts are often hard to predict, and may only occur after serious personal damage is already done. Eventually, the individual’s problem spreads and becomes someone else’s problem—or a

problem for the entire company.

These risks are not limited to security leaders exclusively. They are shared by people in high-stress occupations in every industry. Cybersecurity team members also feel it—63% of respondents say their team experiences “alert fatigue” that desensitizes them to the urgency of security events.

6

Organizations can do more to support security leaders

Cybersecurity leaders depend on their employers for support and alignment on core strategic initiatives. Respondents reported looking towards senior leadership to increase security budgets so the organization can afford the tools it needs to address cybersecurity threats.

US-based respondents also report seeking reassurance on job security. Many organizations lack formal policies describing security leaders' personal liability when addressing cyberattack risks. When incidents occur, it is tempting for stakeholders to assign blame entirely on the security leader. This may happen even when the incident could have been mitigated with technology that the leader requested, but the board denied.

One of the key takeaways of our report showcases the importance of developing a positive work culture around security topics and investments. Instead of seeing security initiatives as cost centers that don't generate revenue, organizations must see cybersecurity for what it truly is—a team sport, with responsibilities shared by every member of the organization.

7

Cybersecurity leaders routinely put in overtime

98% of security leaders report working beyond their contracted time. On average, they work 9 extra hours per week. 15% of respondents report working more than 16 hours over their contracted time per week.

The average number of overtime hours worked is even higher in some industries. Security leaders working in the Transport, Utilities, and Telecommunications sectors report working an average of 13 hours' overtime per week. With only two out of every 100 cybersecurity leaders working

within their contracted time, the need for better time and stress management is paramount. Security leaders need more reliable tools and access to scalable resources – either from within the company or through third-party managed security service providers.

8

Practical stress support goes a long way

Cybersecurity leaders who report being offered practical stress management support also tend to report having a good relationship with their organization's senior leaders. They are less likely to report strategic misalignment on core priorities and less likely to actively search for new roles at other companies.

For organizations, implementing stress management and well-being initiatives can materially improve working conditions for people in high-stress leadership positions like CISOs. Incorporating stress management and work/life boundaries into C-suite schedules can have a profoundly positive impact on job satisfaction.

Our survey shows that it's never too late to implement practical stress support. 63% of respondents say their relationship with the Board has

improved over the past 12 months. Of these, 73% report being offered practical support to manage stress.

Starting with practical support for stress management is a good way for senior leaders to help security decision-makers to generate real value for the organization. Granting them the power to make positive changes to workplace security enhances the organization's ability to manage risk and prevent cyberattacks consistently over time.

9

Reduce stress while improving operational security performance

Our report provides a few valuable insights for security leaders and stakeholders facing obstacles to security performance:

- Security operations already involve high levels of stress and risk. Supporting security personnel and equipping them with the appropriate tools is vital for long-term success.
- Organizations that place personal liability on security leaders may risk losing core personnel as a result. This is especially true when leaders and Board members have a history of conflict.
- Investing in prevention-based security technologies like [Anti Data Exfiltration \(ADX\)](#) can help reduce alert fatigue and streamline security operations. This helps security leaders and board members align their objectives and improve their working relationship with one another.
- Automated and cost-effective solutions like [BlackFog ADX](#) help organizations prioritize cyber resilience while maximizing the value offered by human expertise. Discover how BlackFog can help your organization retain top talent and ensure consistently positive security outcomes.

RESEARCH at-a-glance

Cybersecurity Leaders Under Pressure

BlackFog research shows that stress and overwork are pushing key talent to their limits.

24% of CISOs and IT Security Decision Makers are looking to leave their roles



54% are open to new opportunities



93% say stress and job demands are driving the decision to leave their roles



98% work on average an extra 9 hours per week beyond their contract



45% have used drugs or alcohol to manage stress



42% worry about AI-powered attacks



37% say malware and ransomware cause the most stress

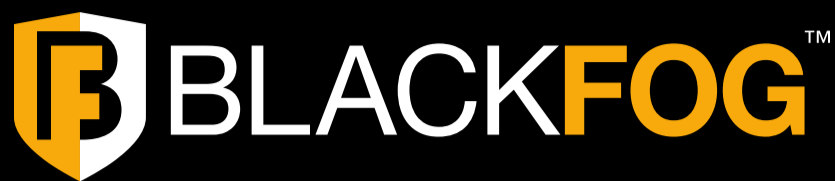


41% want bigger budgets for security tools



METHODOLOGY

The results from this survey are from an online survey Sapio Research fielded on behalf of BlackFog with IT Security Decision Makers in companies of over 500 employees across the UK (200) and US (200). The research was conducted in July and August 2024.



ABOUT BLACKFOG

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

All contents copyright © 2024 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.

[BLACKFOG.COM](https://blackfog.com)